UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/728,396	12/05/2003	Anthony J. Yeates	M61.12-0576	9252

27366 7590 01/07/2008

WESTMAN CHAMPLIN (MICROSOFT CORPORATION)
SUITE 1400
900 SECOND AVENUE SOUTH
MINNEAPOLIS, MN 55402-3319

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
01/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	Application No. 10/728,396	Applicant(s) YEATES ET AL.	
	Examiner LEYNNA T. HA	Art Unit 2135	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 30 November 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☐ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: _____.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

Thanhnga B. Truong

THANHNGA TRUONG
PRIMARY EXAMINER

Continuation of 11. does NOT place the application in condition for allowance because: claims 1 and 3-23 remains rejected in view of Sutter and Nguyen.
Sutter discloses an invention of idependent distributed database (IDDB) where a database comprises a collection of activities that can be collaborated on by various uses at various sites and services that users and sites can selectively use. The IDDBMS provides a mechanism where a site can create a new record and therefore a new key such that the generated key is guaranteed to be unique across the entire database (col.6, lines 43-56). Further, Sutter includes means for securing the information transmitted across the application networks and includes means for ensuring that the application's database can be read and written only through a legitimate application program and by legitimate users (col7, lines 1-66). Therefore, Sutter's invention includes database security.
Examiner traverses the argument on pg.3 of 1st paragraph, that Sutter reference fails to teach or suggest any subsequent utilization of the original encryption component that was combined with the developer password. Claim 1 recites using the password to generate a user specific version of the encryption component, selectively allowing the user to process the user-specific version of the encryption component to derive the encryption component, and using the encryption component to process sensitive data. There are no suggestions that claim 1 include any subsequent utilization of the original encryption component that was combined with the developer password. The use of the password is recited twice where the password is from the user and using the password to generate a user-specific encryption component. Claim 1 fails to recite combining anything with either the encryptio component nor the password.

Examiner traverses the argument on pg.3 of 2nd paragraph, that Sutter does not teach or suggest additional sensitive informaiton is processed using the same encryption or password hash and does not teach using the original encryption component to process sensitive information. Sensitive information is relative to how sensitive and what is considered as sensitive. Thus, sensitive information can broadly be intepreted as any form of data that has protection or does not allow unauthorized person to view/obtain the information. Sutter discloses the application database includes tables which are used by the IDDBMS to store security and other specific information where the tables are needed because the users, permissions, and similar information must be stored and administered separately for each application network (col.40, lines 50-56). Sutter discloses the key or key value (encryption component) is derived from the password which reads on the claimed utilizing the password as a basis for generation of a user-specific encryption component (col.45, lines 45-51). Sutter discusses the key (encryption component) can be used for selectively encrypt contents (col.87, lines 40-43), to decrypt the private signing key to create the signature (col.5, line 20-col.52, line 55). The allocated ID's the IDDBMS will use as keys, and which tables use the keys, the activities and activity parts, along with the basic permissions that apply to each activity, or activity part (col.54, lines 46-60 and col.85, lines 38-67). The ID, password used to derive the key, private key, and permission are all related or given by the user. Thus, Sutter's invention suggests it is specific to a particular user(s). Hence, Sutter processing sensitive data by using the key (to process) to decrypt information to create the signature or the key is used to process certain permissions related to activities or activity parts reads ont the claimed invention.

As for aguments on pg.3-4 for claim 14, refer to the traversal above for claim 1.

Examiner traverses the argument on pg.4 of 2nd paragraph, that Sutter teaches away from comparing the encrypted version of the password to authorized values since Sutter discloses there is no need to store even a hash of the user signing the password. Sutter's hash is not the only data that can be given as the claimed encrypted version. For the claimed encrypted version can broadly interpreted as an encryption key, private key, or key which can also be key values because the key and its value is derived/formed from the password (col.89, lines 32-57 and col.87, lines 44-col.88, line 65). Sutter discloses the IDDBMS can calculate a minimal set of cryptographic keys legitimately required by the user to use the database. The dPermission table inlcudes one record for each basic permission in the database security model and embodies a many-to-many relationship describing the parts of the database covered for each permission. The dKey table includes one record for each cryptographic key used to encrypt any data or stamp column in the database (col.54, lines 46-60 and col.85, lines 38-67). Sutter also discusses the querying the IDDBMS to determine the user's actual permissions for some activity where the actual persmissions are determined by performing in pseudo-code form, ad whether the requested permission is in the result set of the allowed permissions for this user and activity (col.86, lines 28-65 and col.87, lines 44-col.88, line 65). Therefore, Sutter suggests the claimed comparing the encrypted version to a list of authorized values in a database (col.89, lines 32-57 and col.87, lines 44-col.88, line 65).